Definiciones, Teoremas y Propiedades de Álgebra

1. Conjuntos y Lógica

- **Def.:** Llamamos **Conjunto** a una colección de elementos. Decimos que está dado por **Extención** si están listados todos los elementos y que está dado por **Comprensión** si está definido por las propiedades de sus elementos.
- **Def.:** Definimos al **Conjunto Vacío** ϕ como el conjunto que no contiene elementos, es decir, $\phi = \{\}$.
- **Prop.:** El orden de los elementos y la cantidad de veces que se repite alguno en un conjunto no lo afectan.
- **Def.:** Sea A un conjunto y x un elemento decimos que x **Pertenece** a A si x es un elemento de A. Notamos $x \in A$.
- **Def.:** Definimos una **Proposición** como un enunciado cuyo valor lógico solo puede ser verdadero o falso.
- **Def.:** Definimos una **Tabla de Verdad** como una tabla donde se presentan todas las combinaciones posibles de valores lógicos de proposiciones y de operaciones de proposiciones. Notamos el valor lógico verdadero como V o T y el valor lógico falso como F.
- **Def.:** Llamamos a las operaciones lógicas $\neg$ como **Negación**, $\wedge$ como **Conjunción**, $\vee$ como **Disyunción**, $\veebar$ como **Disyunción Exclusiva**, $\implies$ como **implicación** y $\iff$ o $\equiv$ como **Doble Implicación** o **Equivalencia** respectivamente. Estas operaciones se definen de la siguiente forma:

p	q	$\neg p$	$p \wedge q$	$p \vee q$	$p \veebar q$	$p \implies q$	$p \iff q$
V	V	F	V	V	F	V	V
V	F	F	F	V	V	F	F
F	V	V	F	V	V	V	F
F	F	V	F	F	F	V	V

- **Prop.:** Sean p y q proposiciones:
  - $(p \veebar q) \iff ((p \vee q) \wedge \neg(p \wedge q)) \iff ((p \wedge \neg q) \vee (\neg p \wedge q))$.
  - $(p \implies q) \iff (\neg p \vee q)$.
  - $(p \iff q) \iff ((p \implies q) \wedge (q \implies p))$.
- **Def.:** Sean A y B dos conjuntos decimos que A está **Contenido** en B, o que A es un **Subconjunto** de B $\iff$ $x \in B \ \forall x \in A$. Notamos $A \subseteq B$.
- **Prop.:** Sean A y B dos conjuntos $\implies (A \subseteq B) \wedge (B \subseteq A) \iff A = B$.
- **Def.:** Sea A un conjunto definimos el **Conjunto de Partes** de A como el conjunto de todos los subconjuntos de A, es decir, $\mathcal{P}_{(A)} = \{x \ / \ x \subseteq A\}$.
- **Def.:** Sea A un conjunto llamamos su **Cardinalidad** a la cantidad de elementos que pertenecen a A. Notamos $|A|$.
- **Prop.:** Sea A un conjunto $\implies \left|\mathcal{P}_{(A)}\right| = 2^{|A|}$.
- **Def.:** Sean A y B conjuntos definimos la **Unión** de ambos conjuntos como $A \cup B = \{x \ / \ (x \in A) \vee (x \in B)\}$.

- **<u>Def.:</u>** Sean A y B dos conjuntos definimos la **Intersección** de ambos como $A \cap B = \{x \mathbin{/} (x \in A) \wedge (x \in B)\}$. Si $A \cap B = \phi$ los llamamos **Disjuntos**.
- **<u>Def.:</u>** Sean A y B dos conjuntos tales que $A \subseteq B$ definimos al **Complemento** de A como $A' = \{x \mathbin{/} (x \in B) \wedge (x \notin A)\}$.
- **<u>Def.:</u>** Sean A y B dos conjuntos definimos la **Resta** de ambos como $A \backslash B = \{x \mathbin{/} (x \in A) \wedge (x \notin B)\}$.
- **<u>Prop.:</u>** Sean A y B dos conjuntos $\implies A \backslash B = A \cap B'$.
- **<u>Obs.:</u>** Las operaciones de conjuntos complemento, intersección y unión son equivalentes a las operaciones lógicas negación, conjunción y disyunción respectivamente.
- **<u>Leyes de De Morgan</u>**: Sean A y B dos conjuntos:
    - $(A \cup B)' = A' \cap B'$.
    - $(A \cap B)' = A' \cup B'$.
- **<u>Prop.:</u>** Sean A, B y C conjuntos:
    - $(A \cap B) \cup C = (A \cup C) \cap (B \cup C)$.
    - $(A \cup B) \cap C = (A \cap C) \cup (B \cap C)$.
- **<u>Def.:</u>** Sean A y B dos conjuntos definimos la **Diferencia Simétrica** como $A \Delta B = (A \cap B') \cup (A' \cap B)$.
- **<u>Prop.:</u>** Sean A, B y C conjuntos:
    - $A \Delta B = (A \cup B) \backslash (A \cap B)$.
    - $A \cap (B \Delta C) = (A \cap B) \Delta (A \cap C)$.
    - $(A \Delta B) \Delta C = A \Delta (B \Delta C)$.
- **<u>Def.:</u>** Sean A y B dos conjuntos definimos el **Producto Cartesiano** de ambos como $A \times B = \{(x, y) \mathbin{/} (x \in A) \wedge (y \in B)\}$.
- **<u>Def.:</u>** Sean A, B y $\mathcal{R}$ conjuntos llamamos a $\mathcal{R}$ una **Relación** de A en B si $\mathcal{R} \subseteq (A \times B)$. Además, decimos que el elemento x está **Relacionado** con el elemento y si $(x, y) \in \mathcal{R}$. Notamos $x\mathcal{R}y$.
- **<u>Def.:</u>** Sean A un conjunto llamamos a $\mathcal{R}$ una relación de A si $R \subseteq (A \times A)$.
- **<u>Def.:</u>** Sea A un conjunto y $\mathcal{R}$ una relación de A la llamamos:
    - **Reflexiva** $\iff x\mathcal{R}x \ \forall x \in A$.
    - **Simétrica** $\iff (x\mathcal{R}y \iff y\mathcal{R}x) \ \forall x, y \in A$.
    - **Antisimétrica** $\iff ((x\mathcal{R}y \wedge y\mathcal{R}x) \implies x = y) \ \forall x, y \in A$.
    - **Transitiva** $\iff ((x\mathcal{R}y \wedge y\mathcal{R}z) \implies x\mathcal{R}z) \ \forall x, y, z \in A$.
- **<u>Def.:</u>** Sea A un conjunto y $\mathcal{R}$ una relación de A la llamamos una **Relación de Orden** si es reflexiva, antisimétrica y transitiva, y una **Relación de Equivalencia** si es reflexiva, simétrica y transitiva. Si $\mathcal{R}$ es una relación de orden la llamamos **Relación de Orden Total** $\iff (x\mathcal{R}y \wedge y\mathcal{R}x) \ \forall x, y \in A$.
- **<u>Def.:</u>** Sea A un conjunto, $\mathcal{R}$ una relación de equivalencia de A y $x \in A$, llamamos la **Clase de Equivalencia** de x al conjunto $\bar{x} = \{y \in A \mathbin{/} x\mathcal{R}y\}$.
- **<u>Prop.:</u>** Sea A un conjunto y $\mathcal{R}$ una relación de equivalencia de A, $x, y \in A \implies (\bar{x} = \bar{y}) \vee (\bar{x} \cap \bar{y} = \phi)$.
- **<u>Def.:</u>** Sea A un conjunto llamamos una **Partición** de A a un conjunto de subconjuntos disjuntos I cuya unión es A. Es decir, $I = \{A_i\}$, $i \leqslant N$, $i, N \in \mathbb{N}$ es una partición de $A \iff \left((A_i \subseteq A \ \forall i) \wedge (A_i \cap A_j = \phi \ \forall i \neq j) \wedge \left(\bigcup_{i=1}^{N} A_i = A\right)\right)$.

- **Prop.:** Sea A un conjunto y $\mathcal{R}$ una relación de equivalencia de A entonces R da una partición de A en clases de equivalencia.

- **Prop.:** Sea A un conjunto e I una partición de $A \implies \exists\ \mathcal{R}$ relación de equivalencia de $A\ /\ I = \{\bar{x}\},\ x \in A$.

2. Funciones

- **Def.:** Sean A y B conjuntos llamamos una **Función** de A en B a una relación de A en B $f = \{(x, y)\ /\ \forall x \in A \exists!\ y \in B\} \subseteq (A \times B)$. Notamos $f : A \to B$.

- **Def.:** Sea $f : A \to B$ llamamos a A el **Domino** de la función y a B el **Codomino**. Notamos $Dom(f) = A$.

- **Def.:** Sea $f : A \to B$ llamamos la **Imagen** de f al conjunto $Im(f) = \{y \in B : \exists\ x \in A / f_{(x)} = y\} \subseteq B$.

- **Def.:** Sea $f : A \to B$ la llamamos **Inyectiva** $\iff \forall y \in Im(f)\ \exists!\ x \in A\ /\ f_{(x)} = y$. La llamamos **Sobreyectiva** o **Suryectiva** $\iff Im(f) = B$. Si f es inyectiva y suryectiva entonces la llamamos **Biyectiva**.

- **Def.:** Sea $f : \mathbb{N} \to B$ la llamamos una **Sucesión** y notamos $\{f_n\}$ o $f_n,\ n \in \mathbb{N}$.

- **Def.:** Sean $f : A \to B$ y $g : C \to D\ /\ Im(f) \subseteq C$ definimos la **Composición** de f y g como la función $g \circ f : A \to D / (g \circ f)_{(x)} = g_{\left(f_{(x)}\right)}$.

- **Def.:** Sea $f : A \to B$ biyectiva llamamos la **Función Inversa** de f a $f^{-1} : B \to A\ /\ (f \circ f^{-1})_{(x)} = x$.

- **Prop.:** Sean $f : A \to B$ y $g : B \to A\ /\ f \circ g = g \circ f \implies f$ y g son biyectivas y $g = f^{-1}$.

3. Principio de Inducción y Recurrencia

- **Def.:** Sea a_n una sucesión y $N, M \in \mathbb{N}$ llamamos la **Sumatoria** de a_n desde M hasta N a la suma de sus términos entre M y N inclusivos. Notamos $\sum\limits_{n=M}^{N} a_n$.

- **Def.:** Sea a_n una sucesión y $N, M \in \mathbb{N}$ llamamos la **Productoria** de a_n desde M hasta N al producto de sus términos entre M y N inclusivos. Notamos $\prod\limits_{n=M}^{N} a_n$.

- **Def.:** Sea $n \in \mathbb{N}$ llamamos a la función **Factorial** como $n! = \prod\limits_{i=1}^{n} i$.

- **Truco de Gauss:** Sea $N, M \in \mathbb{N} \implies \sum\limits_{n=M}^{N} n = \frac{(N-M+1)(N+M)}{2}$.

- **Serie Geométrica:** Sean $N, M \in \mathbb{N}$, $r \in \mathbb{C}\ /\ |r| < 1 \implies \sum\limits_{n=M}^{N} r^n = \frac{r^M - r^{N-1}}{1-r}$.

- **Def.:** Sea $n \in \mathbb{N}$ llamamos una **Función Proposicional** a una proposición cuyo valor lógico depende del valor de n.

- **Def.:** Sea H un conjunto lo llamamos **Inductivo** si $(1 \in H) \wedge (n \in H \implies (n+1) \in H)$.

- **Prop.:** Sea p_n una sucesión proposicional y $H = \{n \in \mathbb{N}\ /\ p_n\}$ inductivo $\implies H = \mathbb{N}$.

- **Def.:** Sea a_n una sucesión la llamamos una **Sucesión por Recurrencia** si cada valor de la sucesión está definida por algún valor anterior. Es decir, $a_{n+1} = f_{(a_n)}$, donde f es alguna función.

- **Principio de Inducción Completa:** Sea p_n una proposición en n / $(\{p_n\}_{n \leqslant n_0},\ n_0 \in \mathbb{N}$ son verdaderos$) \wedge (\{p_n\}_{n \leqslant h}$ son verdaderos $\implies p_{h+1}$ es verdadero , $h \in \mathbb{N}) \iff p_n$ es verdadero $\forall n \in \mathbb{N}$.

- **Principio de Buen Ordenamiento:** Sea $A \in \mathbb{N},\ A \neq \phi,\ \exists\ n_0 \leqslant n\ \forall n \in A$.

- **Prop.:** Principio de Buen Ordenamiento $\iff$ Principio de Inducción Completa $\iff$ Principio de Iducción.

4. Combinatoria

- **Def.:** Sean A y B conjuntos los llamamos **Equinumerables** si $|A| = |B|$.

- **Prop.:** Sean A y B conjutos equinumerables $\iff\ \exists\ f : A \to B$ biyectiva.

- **Prop.:** Sean A y B conjuntos:
  - $|A \cup B| = |A| + |B| - |A \cap B|$.
  - $A \subseteq B \implies |B| \geqslant |A|,\ |A'| = |B| - |A|$.
  - $|A \times B| = |A||B|$.

- **Prop.:** Sean $\{A_i\},\ i \leqslant N,\ i, N \in \mathbb{N}$ conjuntos $\implies |A_1 \times A_2 \times ... \times A_N| = \prod\limits_{i=1}^{N} |A_i|$.

- **Prop.:** Sean A y B conjuntos entonces hay $2^{|A||B|}$ relaciones de ambos.

- **Prop.:** Sea A un conjunto hay $2^{|A|(|A|-1)}$ relaciones reflexivas.

- **Prop.:** Sean A y B conjuntos hay $|B|^{|A|}$ funciones $f : A \to B$.

- **Prop.:** Sean A y B conjuntos:
  - $f : A \to B$ es inyectiva $\iff |A| \leqslant |B|$.
  - $f : A \to B$ es sobreyectiva $\iff |A| \geqslant |B|$.
  - $f : A \to B$ es biyectiva $\iff |A| = |B|$.

- **Prop.:** Sean A y B conjuntos $/|B| \geqslant |A|$ entonces hay $\frac{|B|!}{(|B|-|A|)!}$ funciones inyectivas $f : A \to B$.

- **Def.:** Sean $n, k \in \mathbb{N},\ k \leqslant n$ llamamos el **Número Combinatorio** a $\binom{n}{k} = \frac{n!}{k!(n-k)!}$.

- **Prop.:** $\binom{n}{k} = \binom{n}{n-k}$.

- **Binomio de Newton:** Sean $x, y \in \mathbb{C},\ n \in \mathbb{N}_0 \implies (x + y)^n = \sum\limits_{k=0}^{n} \binom{n}{k} x^{n-k} y^k$.

5. Números Enteros

- **Def.:** Sean $a, d \in \mathbb{Z},\ d \neq 0$ decimos que d **Divide** a $a \iff \exists!\ k \in \mathbb{Z}\ /\ a = kd$. Notamos $d|a$. Llamamos a d el **Divisor** de a y a a el **Dividendo**.

- **Def.:** Sea $p \in \mathbb{Z}$ lo llamamos **Primo** $\iff p \neq 0 \wedge |p| \neq 1$, y p tiene solo 4 divisores. Si un número no es primo entonces lo llamamos **Compuesto**.

- **Prop.:** Sean $a, b, d \in \mathbb{Z},\ d \neq 0$:
  - $d|a \wedge d|b \implies d|a + b$.
  - $d|a \implies d|ab$.
  - $d|a \implies d^b|a^b$.

- **Def.:** Sean $a, b, d \in \mathbb{Z},\ d \neq 0$ se dice que a es **Congruente** a b **Módulo** $d \iff d|a - b$. Notamos $a \equiv b \pmod{d}$.

- **<u>Prop.:</u>** La congruencia es una relación de equivalencia.
- **<u>Prop.:</u>** Sean $d \in \mathbb{Z},\ d \neq 0,\ \{a_i\},\ \{b_i\} \subseteq \mathbb{Z},\ 1 \leqslant i \leqslant n$:
  - $a_i \equiv b_i \pmod d\ \forall i \implies \sum_{i=1}^{n} a_i \equiv \sum_{i=1}^{n} b_i \pmod d$.
  - $a_1 \equiv b_1 \pmod d \implies b_2a_1 \equiv b_2b_1 \pmod d$.
  - $a_i \equiv b_i \pmod d\ \forall i \implies \prod_{i=1}^{n} a_i \equiv \prod_{i=1}^{n} b_i \pmod d$.
  - $a_1 \equiv b_1 \pmod d \implies a_1^n \equiv b_1^n \pmod d$.
- **<u>Algoritmo de División:</u>** Sean $a, d \in \mathbb{Z}, d \neq 0 \implies \exists! k, r \in \mathbb{Z},\ 0 \leqslant r < d /\ a = kd + r$. Llamamos a k el **Cociente** y a r el **Resto**.
- **<u>Prop.:</u>** Sean $a, d, k, r \in \mathbb{Z},\ d \neq 0,\ 0 \leqslant r < d \ /\ a = kd + r$:
  - $\tilde{r} \equiv r \pmod d,\ 0 \leqslant \tilde{r} < d \implies \tilde{r} = r$.
  - $a \equiv b \pmod d \iff a \equiv r \pmod b \wedge b \equiv r \pmod d,\ b \in \mathbb{Z}$.
- **<u>Teorema de Numeración:</u>** Sean $a, d \in \mathbb{N},\ d \geqslant 2 \implies \exists! n \in \mathbb{N}, \{r_i\} \subseteq \mathbb{N},\ 0 \leqslant r_i < d,\ 0 \leqslant i \leqslant n /\ a = \sum_{k=0}^{n} r_k d^k$.
- **<u>Def.:</u>** Sean $a, b \in \mathbb{Z}$ no ambos nulos definimos el **Máximo Común Divisor** de ambos como el número $d = \max(\mathrm{Div}(a) \cap \mathrm{Div}(b))$, donde $\mathrm{Div}(c)$ es el conjunto de divisores de $c\ \forall c \in \mathbb{Z}$. Notamos $(a : b)$.
- **<u>Algoritmo de Euclides:</u>** Sean $a, b, r \in \mathbb{Z} \ /\ a \equiv r \pmod b \implies (a : b) = (b : r)$.
- **<u>Teorema:</u>** Sean $a, b \in \mathbb{Z}$ no ambos nulos $\implies \exists\ s, t \in \mathbb{Z} \ /\ (a : b) = s \cdot a + t \cdot b$.
- **<u>Prop.:</u>** Sean $a, b \in \mathbb{Z}$ no ambos nulos y $d \in \mathbb{Z},\ d \neq 0 \implies d|a \wedge d|b \iff d|(a : b)$.
- **<u>Prop.:</u>** Sean $a, b \in \mathbb{Z}$ no ambos nulos y $k \in \mathbb{Z},\ k \neq 0 \implies (ka : kb) = |k|(a : b)$.
- **<u>Identidad de Bézout:</u>**: Sean $a, b \in \mathbb{Z}$ no ambos nulos y $d \in \mathbb{Z} \ /\ d \neq 0 \implies (a : b) = d \iff d|a \wedge d|b \wedge \tilde{d}|d\ \forall \tilde{d} \in \mathrm{Div}(a) \cap \mathrm{Div}(b)$.
- **<u>Def.:</u>** Sean $a, b \in \mathbb{Z} \ /\ (a : b) = 1$ los llamamos **Coprimos**. Notamos $a \perp b$.
- **<u>Prop.:</u>** Sean $a, b, c, d \in \mathbb{Z},\ c \neq 0,\ d \neq 0$:
  - $c|a \wedge d|a \wedge c \perp d \implies cd|a$.
  - $c|ab \wedge c \perp a \implies c|b$.
- **<u>Prop.:</u>** Sean $a, b \in \mathbb{Z}$ no ambos nulos $\implies \exists!\ \tilde{a}, \tilde{b} \in \mathbb{Z},\ a \perp b \ /\ a = \tilde{a}(a : b),\ b = \tilde{b}(a : b)$.
- **<u>Prop.:</u>** Sean p un número primo y $a \in \mathbb{N} \ /\ p|a \implies (p : a) = p \vee (p : a) = 1$.
- **<u>Prop.:</u>** Sea $a \in \mathbb{Z} \ /\ |a| > 1 \implies \exists\ p$ primo $/\ p|a$.
- **<u>Teorema Fundamental de la Aritmética:</u>** Sea $n \in \mathbb{Z},\ |n| > 1 \implies \exists!\ \{p_i\}$ primos, $\{r_i\} \subseteq \mathbb{N},\ i \in [1, k] \subseteq \mathbb{N} \ /\ |n| = \prod_{i=1}^{k} p_i^{r_i}$.
- **<u>Lema:</u>** Sean $a, b \in \mathbb{N},\ a = \prod_{i=1}^{n} p_i^{r_i},\ b = \prod_{i=1}^{n} p_i^{l_i},\ p_i$ primos, $r_i, l_i \in \mathbb{N}_0\ \forall i \in [1, n] \subseteq \mathbb{N} \implies (a : b) = \prod_{i=1}^{n} p_i^{\min(r_i, l_i)}$.
- **<u>Def.:</u>** Sean $a, b \in \mathbb{N}$ llamamos el **Mínimo Común Múltiplo** de a y b a $[a : b] = \min(\{n \in \mathbb{N} \ /\ a|n \wedge b|n\})$.
- **<u>Prop.:</u>** Sean $a, b \in \mathbb{N},\ a = \prod_{i=1}^{n} p_i^{r_i},\ b = \prod_{i=1}^{n} p_i^{l_i},\ p_i$ primos, $r_i, l_i \in \mathbb{N}_0\ \forall i \in [1, n] \subseteq \mathbb{N} \implies [a : b] = \prod_{i=1}^{n} p_i^{\max(r_i, l_i)}$

- **Teorema:** Existen infinitos números primos.

- **Teorema de Dirichlet:** Sean $a, k \in \mathbb{N} \ / \ a \perp k \implies \exists$ infinitos p primos / $p \equiv k \pmod{a}$.

- **Lema:** Sean $a, b \in \mathbb{Z}, \ p$ primo $\implies (a+b)^p \equiv a^p + b^p \pmod{p}$.

6. Ecuaciones Diofánticas y de Congruencia

- **Def.:** Llamamos una **Ecuación Diofántica** a una ecuación de la forma $\sum\limits_{k_i,j} a_j \prod\limits_{i=1}^{N} x_i^{k_i} = 0, \ k_i \in [0,n] \subseteq \mathbb{N}_0, \ j \in [1, n^N] \subseteq \mathbb{N}, \ a_j \in \mathbb{Z} \ \forall j, \ n \in \mathbb{N}$. N es la cantidad de variables x_i de la ecuación y n es el **Orden** de la ecuación.

- **Teorema de Wiles:** Sea la ecuación diofántica $x^n + y^n - z^n = 0$ no existen soluciones enteras para $n > 2$.

- **Prop.:** Sean $a, b, c \in \mathbb{Z}, \ a, b$ no nulos entonces la ecuación diofántica $ax + by = c$ admite soluciones enteras $\iff (a:b)|c$.

- **Def.:** Sean dos ecuaciones diofánticas $ax + by = c$ y $a'x + b'y = c'$ con $a, b, c, a', b', c' \in \mathbb{Z}$ las llamamos **Equivalentes** si tienen las mismas soluciones $(x, y) \in \mathbb{Z}^2$. Notamos $ax + by = c \leftrightsquigarrow a'x + b'y = c'$.

- **Def.:** Llamamos a una ecuación diofántica **Homogénea** si $\sum\limits_{k_i,j} a_j \prod\limits_{i=1}^{N} x_i^{k_i} = 0 \leftrightsquigarrow \sum\limits_{k_i,j} a_j \prod\limits_{i=1}^{N} (\lambda x_i)^{k_i} = 0, \ k_i \in [0,n] \subseteq \mathbb{N}_0, \ j \in [1, n^N] \subseteq \mathbb{N}, \ a_j \in \mathbb{Z} \ \forall j, \ n \in \mathbb{N}, \ \lambda \in \mathbb{R}$. En particular, cuando mencionemos de la ecuación diofántica homogénea nos referimos a la ecuación $ax + by = 0$, donde $a, b \in \mathbb{Z}$ no nulos.

- **Prop.:** Sea la ecuación diofántica homogénea el conjunto de soluciones enteras $\mathcal{S}_0 = \{(x, y) \in \mathbb{Z}^2 \ / \ x = b'k, \ y = -a'k, \ k \in \mathbb{Z}\}$, donde $a' = \frac{a}{(a:b)}, \ b' = \frac{b}{(a:b)}$.

- **Teorema:** Sea la ecuación diofántica $ax + by = c, \ a, b, c \in \mathbb{Z}$ no nulos, entonces el conjunto de soluciones enteras es $(\mathcal{S} = \phi \iff (a:b) \nmid c) \veebar (\mathcal{S} = \{(x,y) \in \mathbb{Z}^2 \ / \ (x,y) = (x_0, y_0) + (x_p, y_p)\} \iff (a:b)|c)$, donde $(x_0, y_0) \in \mathcal{S}_0$ y (x_p, y_p) es una solución particular distinta a la homogénea.

- **Def.:** Definimos una **Ecuación Lineal de Congruencia** a una ecuación de la forma $ax \equiv c \pmod{m}$, donde $x \in \mathbb{Z}$ es la variable y $a, c \in \mathbb{Z}, \ m \in \mathbb{N}, \ a \neq 0$.

- **Prop.:** Una ecuación lineal de congruencia tiene soluciones enteras $\iff (a:m)|c$. Sean $a' = \frac{a}{(a:m)}, \ c' = \frac{c}{(a:m)}, \ m' = \frac{m}{(a:m)} \implies ax \equiv c \pmod{m} \leftrightsquigarrow a'x \equiv c' \pmod{m'}$.

- **Teorema:** Sea una ecuación lineal de congruencia con $a \neq 0$ entonces el espacio de soluciones enteras es $(\mathcal{S} = \phi \iff (a:m) \nmid c) \veebar (\mathcal{S} = \{x \in \mathbb{Z} \ / \ x \equiv x_p \pmod{m'}\} \iff (a:m)|c)$, donde x_p es alguna solución particular. Además, $\exists! \ x_p \ / \ 0 \leqslant x_p < m'$.

- **Prop.:** Sea $\{m_i\} \subseteq \mathbb{N}, \ i \in [1,n] \subseteq \mathbb{N}, \ m_i \perp m_j \ \forall i \neq j \implies x \equiv c \pmod{m_i} \ \forall i \leftrightsquigarrow x \equiv c \left(\bmod \prod\limits_{i=1}^{n} m_i\right) \ \forall c \in \mathbb{Z}$.

- **Prop.:** Sean $m, m' \in \mathbb{N} \ / \ m'|m$:

  - $c \not\equiv c' \pmod{m'} \implies \begin{cases} x \equiv c' \pmod{m'} \\ x \equiv c \pmod{m} \end{cases}$ Es incompatible $\forall c, c' \in \mathbb{Z}$.

  - $c \equiv c' \pmod{m'} \implies \begin{cases} x \equiv c' \pmod{m'} \\ x \equiv c \pmod{m} \end{cases} \leftrightsquigarrow x \equiv c \pmod{m} \ \forall c, c' \in \mathbb{Z}$.

- **<u>Teorema Chino del Resto:</u>** Sean $\{m_i\} \subseteq \mathbb{N},\ m_i \perp m_j\ \forall i \neq j,\ \{c_i\} \subseteq \mathbb{Z},\ i \in [1, n] \subseteq \mathbb{N} \implies x \equiv c_i \pmod{m_i}$ tiene soluciones enteras $\forall i$. Además, $x \equiv c_i \pmod{m_i} \leftrightsquigarrow x \equiv x_0 \left(\bmod \prod_{i=1}^{n} m_i\right)$ donde $x_0 \in \mathbb{Z}$ es alguna solución particular. Se tiene entonces que las soluciones enteras son $\mathcal{S} = \left\{x \in \mathbb{Z} \ / \ x \equiv x_0 \left(\bmod \prod_{i=1}^{n} m_i\right)\right\} \wedge \exists! x_0 \ / \ 0 \leqslant x_0 < \prod_{i=1}^{n} m_i$.

- **<u>Pequeño Teorema de Fermat:</u>** Sea p un primo positivo $\implies (a^p \equiv a \pmod{p}) \wedge (p \nmid a \implies a^{p-1} \equiv 1 \pmod{p})\ \forall a \in \mathbb{Z}$. Si algún número no primo cumple con esta propiedad entonces lo llamamos **Pseudoprimo** o **Número de Carmichael**.

- **<u>Prop.:</u>** Sea p un primo positivo, $a \in \mathbb{Z} \ / \ p \nmid a,\ n, r \in \mathbb{N} \ / \ n \equiv r \pmod{(p-1)} \implies a^n \equiv a^r \pmod{p}$.

- **<u>Prop.:</u>** Sean p y q dos primos positivos distintos, $a \in \mathbb{Z} \ / \ a \perp pq \implies a^{(p-1)(q-1)} \equiv 1 \pmod{pq}$. Además, sean $m, r \in \mathbb{N} \ / \ m \equiv r \pmod{(p-1)(q-1)} \implies a^m \equiv a^r \pmod{pq}$.

- **<u>Def.:</u>** Sea $m \in \mathbb{N}$ definimos el conjunto $\mathbb{Z}/m\mathbb{Z} = \{\bar{n} \ / \ n \in \mathbb{N}_0,\ n < m\}$ donde $m\mathbb{Z}$ es la relación de equivalencia de congruencia módulo m. Entonces, $\bar{n} = \{k \in \mathbb{Z} \ / \ k \equiv n \pmod{m}\}$ es la clase de equivalencia de n.

- **<u>Def.:</u>** Se define una **Operación Binaria** como una operación $\star$ que toma dos argumentos para calcular otro. Es decir, sean A, B, C conjuntos entonces $\star : \ A \times B \to C$.

- **<u>Def.:</u>** Sea A un conjunto no vacío y sean $\star$ y $\circ$ operaciones binarias se dice que que el conjunto $(A, \star, \circ)$ es un **Anillo** si cumple las siguientes condiciones:
  - A es **Cerrado** bajo $\star$: $a \star b \in A\ \forall a, b \in A$ (**Magma**).
  - $\star$ es **Asociativa**: $(a \star b) \star c = a \star (b \star c)\ \forall a, b, c \in A$ (**Semigrupo**).
  - $\star$ tiene un **Elemento Neutro**: $\exists n \in A \ / \ a \star n = n \star a = a\ \forall a \in A$ (**Monoide**).
  - $\star$ tiene un elemento **Simétrico**: $\exists b \in A \ / \ a \star b = b \star a = n\ \forall a \in A$ (**Grupo**).
  - $\star$ es **Conmutativa**: $a \star b = b \star a\ \forall a, b \in A$ (**Grupo Abeliano**).
  - A es cerrado bajo $\circ$.
  - $\circ$ es asociativa.
  - $\circ$ es **Distributiva** respecto de $\star$: $(a \circ (b \star c) = (a \circ b) \star (a \circ c)) \wedge ((a \star b) \circ c = (a \circ c) \star (b \circ c))\ \forall a, b, c \in A$.

- **<u>Def.:</u>** Sea $(A, \star, \circ)$ un anillo decimos que es un **Anillo Conmutativo** si cumple la condición de que $\circ$ es una operación conmutativa. Si además $\circ$ contiene un elemento neutro decimos que $(A, \star, \circ)$ es un **Anillo Unitario**. Llamamos al elemento neutro de $\circ$ la **Unidad**.

- **<u>Teorema:</u>** Sea $m \in \mathbb{N}$ y $m\mathbb{Z}$ la relación de equivalencia de congruencia módulo m y sean $+$ y $\cdot$ las operaciones definidas en $\mathbb{Z}/m\mathbb{Z}$ por $\bar{n} + \bar{k} = \overline{n+k},\ \bar{n} \cdot \bar{k} = \overline{nk}\ \forall n, k \in [0, m) \subseteq \mathbb{N}_0 \implies (\mathbb{Z}/m\mathbb{Z}, +, \cdot)$ es un anillo comutativo.

- **<u>Def.:</u>** Sea $(A, \star, \circ)$ un anillo unitario lo llamamos **Anillo de División** si todo elemento de A menos el neutro es **Inversible**, es decir, $\exists b \in A \ / \ a \circ b = b \circ a = u\ \forall a \in A \backslash \{n\}$, donde $u \in A$ es la unidad y $n \in A$ es el elemento neutro. Llamamos a b la **Inversa** de a.

- **<u>Def.:</u>** Sea $(A, \star, \circ)$ un anillo de división si es además un anillo conmutativo entonces llamamos a A un **Cuerpo**.

- **<u>Teorema:</u>** Sea p un primo positivo y $p\mathbb{Z}$ la relación de equivalencia de congruendia módulo p entonces $\mathbb{Z}/p\mathbb{Z}$ es un cuerpo.

7. Números Complejos

- **Def.:** Se define el **Número Imaginario** como $i \notin \mathbb{R} \;/\; i^2 = -1$.
- **Def.:** Se define el **Conjunto Complejo** como $\mathbb{C} = \{a + ib \;/\; a, b \in \mathbb{R}\}$.
- **Def.:** Sea $z \in \mathbb{C},\ a, b \in \mathbb{R} \;/\; z = a + ib$ decimos que esa forma de expresar z es la **Forma Binomial**. Además, definimos $\Re(z) = a$ como la **Parte Real** de z y $\Im(z) = b$ como la **Parte Imaginaria** de z.
- **Def.:** Sea $z \in \mathbb{C},\ z = a + ib$ definimos el **Módulo** de z como $|z| = \sqrt{a^2 + b^2}$.
- **Def.:** Sea $z \in \mathbb{C},\ z = a + ib$ definimos el **Conjugado** de z como $\bar{z} = a - ib$.
- **Prop.:** Sea $z \in \mathbb{C} \implies z\bar{z} = |z|^2$.
- **Def.:** Sea $z \in \mathbb{C}$ definimos la **Forma Trigonométrica** de z como $z = r(\cos(\theta) + i\sin(\theta))$, donde $r = |z|$ y $\theta = \arg(z)$, que llamamos **Argumento** de z.
- **Prop.:** Sea $z \in \mathbb{C} \;/\; z = a+ib = r(\cos(\theta) + i\sin(\theta)) \implies r^2 = a^2+b^2,\ \theta = \begin{cases} \arctan\left(\frac{b}{a}\right) & a > 0 \\ \arctan\left(\frac{b}{a}\right) + \pi & a < 0 \end{cases}$.
- **Fórmula de Euler:** $e^{i\theta} = \cos(\theta) + i\sin(\theta)$.
- **Def.:** Sea $z \in \mathbb{C}$ definimos la **Forma Exponencial** de z como $z = re^{i\theta}$, donde r y θ corresponden a los mismo que los de la forma trigonométrica.
- **Fórmula de de Moivre:** Sea $z \in \mathbb{C} \;/\; z = r(\cos(\theta) + i\sin(\theta)) \implies z^n = r^n(\cos(n\theta) + i\sin(n\theta))\ \forall n \in \mathbb{N}$.
- **Teorema:** Sean $n \in \mathbb{N},\ z = re^{i\theta} \in \mathbb{C} \implies \exists\, \omega_k = r^{\frac{1}{n}} e^{i\phi_k},\ \phi_k = \frac{\theta + 2k\pi}{n},\ k \in [0, n) \subseteq \mathbb{N} \;/\; \omega_k^n = z\ \forall k$.
- **Def.:** Sea $n \in \mathbb{N}$ definimos el conjunto $G_n = \{z \in \mathbb{C} \;/\; z^n = 1\}$.
- **Prop.:** $(G_n, \cdot)$ es un grupo abeliano.
- **Prop.:** Sean $n \in \mathbb{N},\ z \in G_n$:
  - $|z| = 1$.
  - Sea $m \in \mathbb{Z} \;/\; n|m \implies z^m = 1$.
  - Sean $m, m' \in \mathbb{Z} \;/\; m \equiv m' \pmod{n} \implies z^m = z^{m'}$.
  - $z^{-1} = \bar{z} = z^{n-1}$.
- **Prop.:** Sean $n, m \in \mathbb{N}$:
  - $n|m \iff G_n \subseteq G_m$.
  - $G_n \cap G_m = G_{(n:m)}$.
- **Def.:** Sea $n \in \mathbb{Z}$ llamamos a $z \in \mathbb{C}$ la **Raíz n-ésima de la Unidad** si $G_n = \{z^k, k \in [0, n) \subseteq \mathbb{N}\}$.
- **Prop.:** Sean $n \in \mathbb{N}$ y $z \in \mathbb{C}$ entonces z es una raíz n-ésima de la unidad si $z^m = 1 \iff n|m\ \forall m \in \mathbb{Z}$.

8. Polinomios

- **Def.:** Sea K un cuerpo y $n \in \mathbb{N}_0$ decimos que f es un **Polinomio** con coeficientes en K si $f = \sum\limits_{i=1}^{n} a_i X^i, \ a_i \in K \ \forall i, \ a_n \neq 0$, donde X es una indeterminada sobre K. Notamos $f \in K[X]$. Llamamos a los a_i **Coeficientes** de f y a n el **Grado** de f, notamos $\text{Gr}(f)$. Llamamos a a_n el **Coeficiente Principal** de f y lo notamos $\text{Cp}(f)$.
- **Prop.:** Sean $f, g \in K[X]$:
  - $\text{Gr}(f+g) \leqslant \text{máx}\,(\text{Gr}(f), \text{Gr}(g))$.
  - $\text{Gr}(f+g) = \text{máx}\,(\text{Gr}(f), \text{Gr}(g)) \iff (\text{Gr}(f) \neq \text{Gr}(g)) \vee (\text{Cp}(f) \neq -\text{Cp}(g))$.
- **Def.:** Sea $f \in K[X]$ lo llamamos **Mónico** si $\text{Cp}(f) = 1$.
- **Def.:** Sean $f, g \in K[X], \ g \neq 0$ decimos que g **Divide** a $f \iff \exists \ q \in K[x] \ / \ f = q \cdot g$. Notamos $g|f$ y en caso contrario notamos $g \nmid f$.
- **Prop.:** Sean $f, g \in K[X] \ / \ g|f$, si $f|g \vee \text{Gr}(f) = \text{Gr}(g) \implies \exists c \in K \ / \ f = cg$.
- **Def.:** Llamamos a $f \in K[X]$ **Irreducible** si $f \notin K$ y si sus divisores son de la forma $g = c$ o $g = cf$, donde $c \in K$.
- **Teorema:** Sean $f, g \in K[X] \implies \exists! \ q, r \in K[X] \ / \ f = q \cdot g + r$ con $r = 0$ o $\text{Gr}(r) < \text{Gr}(g)$.
- **Def.:** Definimos el **Máximo Común Divisor** entre dos polinomios como el polinomio mónico de mayor grado que divide a ambos.
- **Teorema:** Sea $f \in K[X], \ \text{Gr}(f) \geqslant 1 \implies \exists \ c \in K, \ g_n \in K[X], \ m_n \in \mathbb{N}, \ n \in [1, r] \subseteq \mathbb{N}$ mónicos $/ \ f = c \prod\limits_{i=1}^{r} g_n^{m_n}$.
- **Def.:** Sea $f \in K[X]$ definimos la **Función Evaluación** como la función $f : K \to K$ que evalúa al polinomio f en algún punto $x \in K$, es decir, $f(x) = \sum\limits_{i=1}^{n} a_i x^i$.
- **Def.:** Sea $f \in K[X]$ definimos una **Raíz** de f a algún punto $x \in K \ / \ f(x) = 0$.
- **Prop.:** Sea $f \in K[X], \ x \in K$ es raíz de $f \iff X - x|f \iff \exists \ q \in K[X] \ / \ f = q(X - x)$.
- **Prop.:** Sean $f, g \in K[X], \ x \in K$, entonces $f(x) = 0 \wedge g(x) = 0 \iff (f : g)(x) = 0$
- **Def.:** Sea $f \in K[X], x \in K$ una raíz de f definimos su **Multiplicidad** como $m \in \mathbb{N} \ / \ (X - x)^m | f \wedge (X - x)^{m+1} \nmid f$.
- **Def.:** Sea $f \in K[X], x \in K$ una raíz de f la llamamos **Múltiple** si también es raíz de la derivada de f. Si no lo es, la llamamos **Simple**.
- **Prop.:** Sea $f \in K[X], \ \text{Gr}(f) = n, \ x_i \in K$ raíces de f con multiplicidad $m_i, \ i \in [1, r] \subseteq \mathbb{N} \implies \sum\limits_{i=1}^{r} m_i \leqslant n$.
- **Teorema Fundamental del Álgebra:** Sea $f \in \mathbb{C}[X], \ \text{Gr}(f) = n \geqslant 1 \implies \exists \ z_i \in \mathbb{C}, \ m_i \in \mathbb{N}, \ i \in [1, r] \subseteq \mathbb{N}$ raíces de $f \ / \ \sum\limits_{i=1}^{r} m_i = n$.
- **Prop.:** Sea $f \in \mathbb{C}[X], \ z \in \mathbb{C}$ una raíz de f de multiplicidad $m \implies \bar{z}$ es una raíz de f de multiplicidad m.